**Nội dung và hướng dẫn bài thực hành**

***Mục đích***

Giúp sinh viên làm quen với gói tin chuẩn wifi tốc độ cao và tiếp cận các bộ lọc về loại gói tin này. Đồng thời cung cấp kiến thức về mạng chuẩn 802.11ac.

**Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về Wireshark.

***Nội dung thực hành***

Khởi động bài lab:

Vào terminal, gõ:

*labtainer -r 802-11ac*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong terminal student ảo sẽ xuất hiện.

Gõ lệnh: *wireshark*để khởi động wireshark.

Sau đó sinh viên tìm kiếm kết quả cho các câu hỏi sau:

* Task 1: Tìm BSSID chịu trách nhiệm chính cho SSID “myhotspot”, có bao nhiêu gói tin theo chuẩn 802.11ac được truyền qua BSSID này.
* Khi thiết bị khách được kích hoạt hoặc thay đổi bộ dịch vụ cơ sở (BSS - Base Service Set), nó sẽ phát đi gói tin probe request với tên SSID của điểm truy cập trong danh sách mạng đã lưu. Nếu SSID của thiết bị phát Wi-Fi  trong mạng khớp với SSID đó, nó sẽ phản hồi bằng gói tin probe response. Do đó, để đảm bảo kết nối liền mạch cho thiết bị khách, các mạng lớn sẽ gán nhiều BSSID cho 1 SSID.
* Cách làm: Trên thanh menu, chọn Wireless → WLAN Traffic . Nó sẽ mở một cửa sổ mới với tất cả lưu lượng được nhóm theo BSSID. Trên Display filter, sử dụng bộ lọc:

*wlan.ssid==”myhotspot”*

* Sau khi thấy được BSSID chịu trách nhiệm chính (Có percent Package cao nhất), chuột phải → Apply as Filter → Selected để hiển thị toàn bộ những gói tin BSSID này đã truyền.
* Để tìm lọc ra những gói tin theo chuẩn 802.11ac, thêm vào bộ lọc lệnh phy (mã loại chuẩn 802.11ac là 8):

*wlan\_radio.phy == 8*

* Xem số lượng gói tin được hiển thị và trả lời theo dạng:

*(BSSID), (số lượng gói tin)*

* Task 2: Có bao nhiêu thiết bị khách hàng được kết nối với BSSID 44:f0:21:54:3a:67 tại  MAC timestamp: 292591157?
* MAC timestamp là một trường trong Wifi frame, thường được sử dụng để ghi lại thời gian chính xác mà một sự kiện cụ thể xảy ra trên lớp MAC (Medium Access Control). Thông số này thường được ứng dụng cho việc đồng bộ thời gian.
* MAC timestamp nằm trong phần RadioTap Header của gói tin.
* Sử dụng bộ lọc:

*wlan.bssid==44:f0:21:54:3a:67 && radiotap.mactime == 292591157*

* Task 3: Có bao nhiêu gói tin nào trong lưu lượng được thu thập được truyền bằng cách sử dụng 802.11ac beamforming?
* Thông thường tín hiệu Wi-Fi được phát sóng theo mọi hướng bằng các ăng-ten đa hướng (omni-directional antennas). Tuy nhiên, có những loại ăng-ten đặc biệt có thể chỉ hướng tín hiệu đến thiết bị nhận, làm tăng công suất tín hiệu và cho phép truyền tải nhanh hơn do giảm thiểu lưu lượng truy cập, 802.11ac beamforming là một trong số đó.
* Sử dụng bộ lọc:

*wlan\_radio.11ac.beamformed*

* Task 4:  Có bao nhiêu gói tin của BSSID 04:f0:21:54:3a:67 được truyền với MCS9?
* **MCS (Modulation and Coding System)** là hệ thống làm rõ tốc độ dữ liệu trên một loạt các băng thông kênh, guard intervals, và spatial streams. Trong 802.11ac, có 10 chỉ số MCS, từ 0 đến 9. Nói một cách đơn giản, chỉ số MCS càng cao thì chất lượng truyền/nhận dữ liệu càng tốt.
* Sử dụng bộ lọc:

*wlan.bssid == 04:f0:21:54:3a:67 && wlan\_radio.11ac.mcs == 9*

* Task 5: Tìm giá trị công suất phát tối đa của Access Point lưu trữ SSID “myhotspot”(đơn vị dBm, làm tròn 1 số sau dấu phẩy).
* Công suất phát của Access Point(AP) là mức năng lượng được sử dụng để truyền tín hiệu không dây từ AP đến các thiết bị nhận, được đo bằng decibel-milliwatts (dBm) hoặc milliwatt (mW)
* Công suất phát của mỗi thiết bị phần cứng là cố định, giá trị này nằm trong Beacon frame's tagged (195). Để có được dữ liệu này, sử dụng bộ lọc và tìm tham số Tx (truyền) Power Envelope:

*wlan.ssid == "myhotspot" && wlan.fc.type\_subtype == 0x8*

*&& wlan.tag.number == 195*

* Vì được phát cùng thiết bị nên ta có thể thấy rằng tất cả các kênh tần số đều có cùng giá trị.
* Trả lời theo dạng: (*Đáp án)* dBM

* Task 6: Điểm truy cập có BSSID 04:f0:21:54:3a:67 có hỗ trợ SU-Beamforming hoặc MU-Beamforming không?
* Beamforming của thiết bị WiFi:
* Hướng đến một máy khách duy nhất: Beamforming single-user (SU).
* Hướng đến nhiều máy khách: Beamforming multi-user (MU).
* Thông tin này có thể được tìm thấy trong beacon’s frame tagged (191). Lọc lưu lượng theo BSSID và số thẻ 191:

*wlan.bssid == 04:f0:21:54:3a:67 && wlan.tag.number == 191*

* VHT (Very High Throughput) Capabilities là một tập hợp các tính năng nhằm cải thiện tốc độ và hiệu suất mạng không dây dành cho chuẩn 802.11ac. Các tính năng này được thiết kế để đạt hiệu năng cao hơn so với chuẩn 802.11n (HT – High Throughput). Cả 2 đều nằm trong dữ liệu Beacon Frame

* Trả lời theo dạng sau:

SU: *YES/NO*, MU: *YES/NO*

* Kiểm tra kết quả:
* Sinh viên tạo 1 file và lưu kết quả vào 5 dòng khác nhau với định dạng:

Task *x:*(*Kết quả*)

* Lệnh tạo file:

*nano tên\_file*

* Thực hiện biên dịch chương trình result.c và chạy:

*gcc result.c -o result*

*./result*

* Sau khi chạy chương trình, nhập tên file chứa đáp án vào để kiểm tra kết quả.

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.